CHAPTER 10-13-06
SECURITY OF CRIMINAL HISTORY RECORD INFORMATION

Section

10-13-06-01. Policies and procedures required. All criminal justice agencies maintaining criminal history record systems, whether manual or automated must have written policies and procedures to protect criminal history data from unauthorized access. Written policies and procedures will include at a minimum:

1. Designation of personnel authorized access to criminal history files.

2. Screening of personnel authorized access.

3. Screening of noncriminal justice personnel with indirect access or work proximity to criminal history files (such as computer programmers, maintenance personnel, and nonagency janitorial personnel).

4. Supervision of personnel with direct or indirect access or proximity to criminal history files.

History: Effective November 1, 1987.
General Authority: NDCC 12-60-16.3
Law Implemented: NDCC 12-60-16.3

10-13-06-02. Facilities. All criminal justice agencies maintaining criminal history record systems, whether manual or automated, must have adequate facilities to protect criminal history data from unauthorized access. Buildings and rooms used for file maintenance should be constructed and utilized so as to prevent unrestricted physical access by unauthorized persons.

History: Effective November 1, 1987.
General Authority: NDCC 12-60-16.3
Law Implemented: NDCC 12-60-16.3

10-13-06-03. Automated systems. Criminal justice agencies operating automated criminal history record systems must provide the following:

1. Protection against unauthorized access.

2. Protection against tampering or destruction.

3. Detection and logging of unauthorized access attempts.

4. Protection of software.

5. Assurance of restricted access in a shared computer system.

History: Effective November 1, 1987.
General Authority: NDCC 12-60-16.3
Law Implemented: NDCC 12-60-16.3